

Databehandleravtale

Vedlegg til Hovedavtalen for abonnement på Compliance Dashbordet

1. Generelt

- 1.1 Denne databehandleravtalen regulerer rettigheter og forpliktelser som gjelder for Compliance Support AS (databehandler/Leverandør) sin behandling av personopplysninger på vegne av Behandlingsansvarlig (Kunde).
- 1.2 Leverandøren skal sikre etterlevelse av Artikkel 28 (3) i EUs Personvernforordning (forordning (EU) 2016/679 - GDPR), jf. personopplysningsloven av 15.06.2018 § 1.
- 1.3 Databehandleravtalen skal også regulere databehandlers behandling av personopplysninger på vegne av Kunde i henhold til DORA (EU) 2022/2554 og tilhørende ITS 2024/2956.
- 1.4 Denne databehandleravtalen skal ses i sammenheng med den Hovedavtalen som er inngått mellom partene. Behandlingen av personopplysninger gjelder slik behandling som er nødvendig for oppfyllelse av avtalen med Kunden.
- 1.5 Databehandleravtalen og Hovedavtalen er avhengig av hverandre og kan derfor ikke sies opp separat. Databehandleravtalen kan bare erstattes av ny og oppdatert databehandleravtale som blir gjort kjent for Kunde per e-post eller signert av begge Parter dersom Kunden krever det.
- 1.6 Ved opphør av avtalen mellom partene har Kunden adgang til å arkivere alle rapporter som er produsert i produktet og som er basert på de data som Kunden har lagt inn i produktet. Deretter skal Leverandøren slette data i produktet som er benyttet av Kunden. Sletting skal gjennomføres innen 60 dager etter opphør av avtalen om ikke annet er skriftlig avtalt med Kunden.

Sletting skal gjennomføres som beskrevet her med mindre annen lovgivning eller avtale mellom partene krever at personopplysningene lagres.
- 1.7 Produktet
Leverandøren utvikler og leverer Compliance Dashbordet (produktet) som er web basert program som Kunden kan benytte etter inngåelse av avtale om abonnement. Dashbordet gir Kunden hjelp med å gjennomføre, holde oversikt over og rapportere internt status, risiko, avvik og tiltak som følge av lov og forskrift eller interne krav hos Kunden.
- 1.8 Hvilke personopplysninger som behandles.
De personopplysningene som Leverandøren behandler personopplysninger om er navn, telefonnummer og e-post til kontaktperson og ansvarlig for signering av Hovedavtalen på vegne av Kunden. I tillegg behandler Leverandøren navn, telefonnummer og e-post til de personer hos Kunden som skal ha tilgang til produktet.

- 1.9 Leverandøren behandler også personopplysninger som er registrert i produktet av Kunden gjennom regelmessig support eller vedlikehold av produktet for Kunden.
- 1.10 Leverandørens behandling av personopplysninger utføres som ledd i oppfyllelse av partenes avtale. Leverandøren kan bare behandle slike personopplysninger som er nødvendig for å oppfylle avtalen med Kunden. Eventuelle løpende instruksjoner fra Kunden skal også gi Leverandøren adgang til å behandle personopplysninger på vegne av Kunden.

Behandlingsoversikten fremgår av Vedlegg A.

2. Rettigheter og forpliktelser for Kunden (behandlingsansvarlig)

- 2.1. Kunden er ansvarlig for at behandlingen av personopplysninger skjer i henhold til personopplysningsloven.
- 2.2. Kunden har rett til, og en forpliktelse til å stadfeste formålet med behandlingen og de midlene som skal benyttes ved behandlingen av personopplysninger.
- 2.3. Kunden har rett til å be Leverandøren om bistand til support eller bruk og utvikling av Dashbordet. Slik bistand kan medføre at Leverandøren får kjennskap til personopplysninger hos Kunden. Personopplysninger som Leverandøren kan behandle i slike tilfeller kan være navn på ansatte hos Kunden eller kundedata som Kunden har lagt inn i produktet.
- 2.4. Leverandøren skal på forespørsel, med mindre konfidensialitet eller taushetsplikt er til hinder for det, gi Kunden nødvendig informasjon for å dokumentere etterlevelse av GDPR artikkel 28 og denne databehandleravtalen, samt tillate og bidra til revisjoner, herunder gjennomgang utført av Kunden eller av en tredjepart utpekt av Kunden.
- 2.5. Kundens undersøkelser av underdatabehandlere, dersom det er aktuelt, skal som hovedregel gjennomføres av Leverandøren om ikke annet er skriftlig avtalt mellom partene.
- 2.6. Kunden har rett til å motta revisjonsrapporter og gjennomføre revisjoner hos Leverandøren.
- 2.7. Kunden er ansvarlig for å sørge for at behandlingen av personopplysninger som databehandler er instruert om å gjøre, er i samsvar med norsk rett.

3. Forpliktelser for Leverandøren (databehandler)

- 3.1. Leverandøren er bundet av taushetsplikt i behandlingen av personopplysninger, som angitt i Hovedavtalen mellom partene eller i eventuelle skriftlige tilleggsavtaler som partene har inngått.
- 3.2. Leverandøren behandler kun personopplysninger på vegne av Kunden som behandlingsansvarlig basert på partenes avtale eller etter instruksjoner

fra Kunden, med mindre behandlingen er påkrevet etter norsk rett.

- 3.3. Leverandøren behandler personopplysninger som beskrevet i pkt. 1.8 – 1.10. Behandlingen er nødvendig for å oppfylle avtalen med Kunden eller for å oppfylle dokumenterte instruksjoner fra Kunde.
- 3.4. Leverandøren skal uten opphold informere Kunden dersom instruksjoner som er gitt av Kunden er i strid med personopplysningsloven.
- 3.5. Leverandøren skal iverksette egne tekniske og organisatoriske tiltak som beskrevet i Vedlegg B og bistå Kunden ved rettighetsforespørsler, DPIA eller tilsyn.
- 3.6. Ved oppdagelse av brudd på personopplysnings-sikkerheten ved Leverandørens fasiliteter, eller hvor det er relevant – en underdatabehandlers fasiliteter, skal Leverandøren uten opphold varsle Kunden.
- 3.7. Tatt i betraktning behandlingens art og de tilgjengelige data, skal Leverandøren bistå Kunden i rapporteringen av bruddet til Datatilsynet.
- 3.8. Leverandøren skal oppfylle krav til operasjonell robusthet, leverandørstyring og hendelseshåndtering som beskrevet i SLA til avtalen mellom partene.

4 Sikkerhet ved behandling av personopplysninger

- 4.1. Leverandøren skal treffe tiltak som kreves i henhold til GDPR Artikkel 32. Partene skal derfor iverksette hensiktsmessige tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er tilpasset risikoen. Som hovedregel benytter Leverandøren seg av passordbeskyttelse (kryptering) ved oversendelse av personopplysninger og kryptering av det utstyret som benyttes til behandling av personopplysninger.

- 4.2. Eventuelle sikkerhetstiltak kan endres i løpet av avtaleforholdet.

5 Bruk av underdatabehandlere

- 5.1. Underdatabehandlere benyttes i samråd med de opplysninger som Leverandøren har opplyst om i Hovedavtalen, SLA til Hovedavtalen eller denne databehandleravtalen. Godkjente underdatabehandlere fremgår av Vedlegg C.
- 5.2. Endringer i bruk av underdatabehandlere skal varsles til Kundens kontaktperson minst 30 dager før endringen iverksettes. Kunden har rett til å protestere. Eventuell protest på bruk av underdatabehandler skal sendes fra Kunden til Leverandøren per e-post til: hello@governance.no
- 5.3. Når en annen databehandler opptrer som underdatabehandler engasjert av Leverandøren, skal Leverandøren oppfylle kravene fastsatt i GDPR artikkel 28 nr. 2 og 4.
- 5.4. Dersom Leverandøren engasjerer en ny underdatabehandler, skal Kunden varsles. Kunden må gi sitt samtykke før eventuelle underdatabehandlere kan behandle personopplysninger.

6 Overføring av personopplysninger til tredjestater

- 6.1. Det overføres ingen personopplysninger utenfor EU/EØS. Appfarm AS som er Leverandørens underdatabehandler som opplyst i vedlegg C, benytter datasenter innenfor EU/EØS.

Vedlegg A – Behandlingsoversikt

Tjeneste: Leverandøren utvikler og leverer Compliance Dashbordet (produktet) som er web basert program som Kunden kan benytte etter inngåelse av avtale om abonnement.

Formålet: Dashbordet gir Kunden hjelp med å gjennomføre, holde oversikt over og rapportere internt status, risiko, avvik og tiltak som følge av lov og forskrift eller interne krav hos Kunden.

Behandlingsaktiviteter: Lagring av data i produktet som Kunden abonnerer på.

Kategorier av registrerte: Ansatte hos Kunden, herunder brukere av produktet og sluttkunder i form av navn på Kundens egne kunder som er lagt inn i produktet.

Kategorier av personopplysninger: Navn, telefonnummer og e-post til kontaktperson og ansvarlig for signering av Hovedavtalen på vegne av Kunden. I tillegg behandler Leverandøren navn, telefonnummer og e-post til de personer (ansatte) hos Kunden som skal ha tilgang til produktet. Leverandøren kan også personopplysninger som er registrert i produktet av Kunden gjennom regelmessig support, vedlikehold eller etter instruks fra Kunden. Dette kan være navn på ansatte og sluttkunder hos Kunden, dvs. Kundens kunde.

Varighet: Personopplysninger lagres i den perioden Kunde har avtale med Leverandøren.

Systemer: Microsoft 365, Datasenter som benyttes av Appfarm AS (Appfarm Plattform). Backup Policy for Appfarm finnes her: <https://policies.appfarm.io/service-and-usage/backup-policy>

Dataplassering: EU/EØS

Vedlegg B – Tekniske og organisatoriske tiltak

De tekniske og organisatoriske sikkerhetstiltakene med Appfarm AS som leverandør av SaaS/hosting fremgår blant annet av Appfarms ISO 27001:2022-sertifisering, Google Cloud Platform som underliggende infrastruktur, og dokumentert backup-modell. Oppdatert compliance-dokumentasjon, sertifikater og policy-dokumenter er tilgjengelig på trust.appfarm.io.

Tilgangskontroll: Appfarm benytter rollebasert tilgangsstyring basert på prinsippet om minste privilegium og «need-to-know». Tilgang til kundedata og systemer gis kun til autorisert personell med tjenstlig behov. Administrativ tilgang er særskilt begrenset og underlagt streng kontroll. Autentisering støttes via sikre mekanismer, og MFA er obligatorisk for all intern administrativ tilgang. For kundens egne brukere håndheves MFA gjennom kundens identitetsleverandør (f.eks. Microsoft Entra ID) via OIDC.. Tilganger gjennomgås jevnlig og ved endringer i roller eller ansettelsesforhold. Alle tilganger og privilegerte handlinger loggføres. Tilgangsstyringen understøttes av underliggende cloud-plattform (Google Cloud) og interne kontrollrutiner.

Kryptering: Appfarm sikrer konfidensialitet og integritet av data gjennom kryptering. Data i transitt er kryptert ved bruk av TLS eller tilsvarende oppdatert protokoll. Data i ro lagres kryptert i underliggende infrastruktur (Google Cloud). Krypteringsnøkler håndteres som standard gjennom Google Clouds nøkkelhåndteringstjeneste (KMS) med Google-managed encryption (AES-256). For kunder med behov for customer-managed encryption keys (CMEK) tilbys dette på Dedicated-abonnementsnivå med dedikert KMS hos GCP, AWS eller Azure. Tilgang til nøkkelmateriale er begrenset og underlagt tilgangskontroll og logging.. Tilgang til nøkkelmateriale er begrenset og underlagt tilgangskontroll og logging.

Logging og overvåking: Appfarm benytter logging og overvåking for å sikre sporbarhet og oppdage sikkerhetshendelser. Sikkerhetsrelevante hendelser, inkludert innlogging, endringer og administrative handlinger, loggføres. Logger beskyttes mot manipulering og oppbevares i henhold til definerte retentionsperioder. Det benyttes overvåkings- og varslingsmekanismer for å identifisere unormal aktivitet. Sikkerhetshendelser håndteres i henhold til etablerte prosedyrer for hendelseshåndtering.

Sårbarhetshåndtering: Appfarm har etablert prosesser for håndtering av sårbarheter. Plattform og underliggende komponenter oppdateres fortløpende med sikkerhetsoppdateringer. Appfarm gjennomfører årlige tredjeparts sikkerhetsrevisjoner (whitebox-tester med tilgang til skymiljøet), pluss løpende sårbarhetsskanning gjennom Google Cloud Security Command Center. Identifiserte sårbarheter risikovurderes og utbedres innen hensiktsmessige tidsfrister. Appfarm benytter også kontroller og sikkerhetsmekanismer i underliggende cloud-plattform.

Backup og recovery: Appfarm gjennomfører regelmessig sikkerhetskopiering av systemer og data. Backup utføres automatisert og periodisk. Data lagres med definerte retentionsperioder. Gjenoppretting (restore) kan gjennomføres på forespørsel fra behandlingsansvarlig. Backup og restore-prosesser testet regelmessig. Backup Policy for Appfarm finnes her: <https://policies.appfarm.io/service-and-usage/backup-policy>

Kontinuitet: Appfarm har etablert tiltak for å sikre tilgjengelighet og håndtering av avbrudd. Tjenesten driftes på en robust cloud-infrastruktur (Google Cloud) med høy grad av redundans. Det foreligger beredskaps- og hendelseshåndteringsprosesser. Gjenoppretting etter hendelser skjer i henhold til etablerte prosedyrer. Backup-mekanismer understøtter gjenoppretting ved datatap. Det er ikke eksplisitt garantert RTO/RPO i standardtjenesten, utover det som følger av backup-oppsett og avtale. Konkrete RTO/RPO-verdier kan avtales på Dedicated-abonnementsnivå..

Vedlegg C – Underdatabehandlere

Kunden har rett til å motta informasjon om samtlige databehandlere som Leverandøren benytter ved behandling av personopplysninger på vegne av Kunden.

Leverandøren benytter følgende underdatabehandlere:

- **Risikonsulenten AS**, org. nr. 920 018 793, adresse: Kleivabergsbakken 45, 4326 Sandnes - ivaretar sentrale funksjoner som supportfunksjon, etablering av Compliance Dashbordet for kunder, opplæring av Kundens representant, oppdatering av innholdet, salg og markedsføring og andre oppgaver som står i forbindelse med administrative oppgaver.
- **Compliance advisor – Erling Grimstad AS**, org. nr. 922 600 821, adresse: Gaustadalléen 21, 0349 Oslo - ivaretar sentrale funksjoner som supportfunksjon, etablering av Compliance Dashbordet for kunder, opplæring av Kundens representant, oppdatering av innholdet, salg og markedsføring og andre oppgaver som står i forbindelse med administrative oppgaver.
- **Appfarm AS**, org. nr. 919 697 199, adresse: Universitetsgata 2, 0164 Oslo som leverandør av Appfarm Plattform der data for Kundens Compliance Dashbord oppbevares.
- **Zebra Consulting AS**, org. nr. 917 700 915, adresse: Tullins gate 4C, 0166 Oslo – ivaretar supportfunksjonen og utvikling av etter oppdrag fra Compliance Support AS.
- **Microsoft Norge AS**, org. nr. 957 485 030, adresse: Dronning Eufemias gate 71, 0194 Oslo – leverandør av Microsoft Office 365.

Standard databehandleravtale for anvendelse av
Compliance Dashbordet er sist oppdatert i juni 2026.

Compliance Support AS, Gaustadalléen 21, 0349 Oslo